UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

BETZALEL YOCHANAN, individually and on behalf of all others similarly situated, Plaintiff(s), v. EQUIFAX, INC., and EQUIFAX WORKFORCE SOLUTIONS, a/k/a TALX CORPORATION	No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, BETZALEL YOCHANAN individually and on behalf of the classes defined below, bring this Class Action Complaint ("Complaint") against Equifax, Inc. and Equifax Workforce Solutions, Inc. a/k/a TALX Corporation (collectively, "Equifax" or "Defendants"), and allege as follows:

NATURE OF THE CASE

1. On May 5, 2016, employees of Kroger and its affiliated companies ("Krogers") were advised that Equifax, which provides online access to electronic W-2 forms for Kroger and other groups of companies, was the subject of a data breach, in which unauthorized individuals accessed Equifax's W2-Express website (hereinafter "Data Breach"). Kroger has advised that it believes the unauthorized individuals who accessed the W2-Express website have already used information gained in the breach, including names, addresses, Social Security numbers, alternative identification numbers, wage information, employment information, and other personal information, to file fraudulent tax returns. (*See "Possible Compromised Tax Information Questions & Answers for Current & Former Associates"* form dated May 5, 2016 attached hereto as **Exhibit A.**)

2. Equifax has not commented on the Data Breach, or provided any notification directly to affected individuals at this time.

3. The Data Breach occurred because Equifax failed to implement adequate security measures to safeguarded consumers' Personal Identifying Information ("PII") and willfully ignored *known* weaknesses in its data security, including prior hacks into its information systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a large number of individuals' valuable personal and financial information.

4. Armed with this personal information, identity thieves can commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's

name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other individuals who intend to misuse the information.

5. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a substantial, heightened, and imminent risk of such harm in the future. It cannot be questioned that the PII of Plaintiff and Class Members was taken for the purpose of stealing the identity of Plaintiff and Class Members which has already resulted in and will continue to result in damage to them. Plaintiff and Class Members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's impact on their PII for the remainder of their lives. Going forward, Plaintiff and Class Members anticipate spending considerable time and money for the rest of their lives in order to detect and respond to the impact of the Data Breach.

6. There is a substantial likelihood that Class Members already have or will become victims of identity fraud given the breadth of information about them that is now publicly available. Javelin Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal."

7. As described by Gasan Awad, Vice President, identity and fraud product management for Equifax, "Data breaches are the first step for criminals with intentions to steal and misuse consumer information. Once fraudsters have consumers' private identity information they then take the next step in criminal activity, often committing fraud by opening fraudulent accounts or taking over an existing account. In essence, fraudsters use the personal information obtained from the breaches to apply for credit or benefits or hijack existing accounts, all while acting as the victims."[1]

8. Plaintiff brings this action to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks to recover damages, including actual and statutory damages, equitable relief, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

PARTIES

A. Plaintiff

9. Plaintiff Betzalel Yochanan is a resident of Atlanta, Georgia and was a Georgia citizen during the period of the Data Breach. Plaintiff Yochanan has been an employee of Kroger for six years, and was provided online access to his electronic W-2 forms from Kroger through Defendant's W-2 Express website. Plaintiff Yochanan used the default PIN provided to him for the W-2 Express website. On or around May 5, 2016, Mr. Yochanan received an emailed notification letter from Kroger regarding the Data Breach. As a result of the Data Breach and the substantial risk of identity theft as a result of the Data Breach, Mr. Yochanan enrolled in identity theft protection services at a monthly cost to him of $9.99 per month.

[1] Awad, Gasan, *Device Advice: Keeping Fraudsters from Consumer Info*, http://www.darkreading.com/endpoint/device-advice-keeping-fraudsters-from-consumer-info/a/d-id/1325182 (last accessed May 19, 2016).

B. Defendants

10. Defendant Equifax, Inc. is incorporated in Georgia with its headquarters and principal place of business located at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. It is a citizen of Georgia.

11. Defendant Equifax Workforce Solutions a/k/a TALX Corporation is a wholly owned subsidiary of Equifax Inc., organized under the laws of the State of Missouri with a principal place of business at 11432 Lackland Road, St. Louis, Missouri 63146. Equifax Workforce Solutions a/k/a TALX Corporation does business throughout the State of Georgia, including Fulton County.

12. Equifax is one of the major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, as described by Equifax "[t]he company organizes, assimilates and analyzes data on more than 800 million consumers and more than 88 million business worldwide, and its database includes employee data contributed from more than 5,000 employers."[2] As a credit bureau service, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendants.

14. This Court has personal jurisdiction over Defendants because they maintain their principal place of business in Georgia, regularly conduct business in Georgia, and have sufficient minimum contacts in Georgia. Defendants

[2] *See Equifax Company Profile,* Equifax, http://www.equifax.com/about-equifax/company-profile (last accessed May 19, 2016).

intentionally avail themselves of this jurisdiction by conducting their corporate operations in Georgia.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Equifax is headquartered in this District, it regularly transacts business in this District, and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in this District.

FACTS

A. The Data Breach Compromised the PII of Thousands of Consumers

16. On May 5, 2016 Kroger announced that Equifax systems had been subject to the Data Breach, and that an unknown number of current and former associates' W-2s had been obtained by unauthorized persons. The PII in employee's W-2s includes names, addresses, Social Security numbers, alternative identification numbers, wage information, employment information, and other personal information.

17. Defendant Equifax has yet to acknowledge the breach, or notify victims of the Data Breach.

18. According to a Kroger spokesman, other companies which rely upon Equifax for W-2 services may have also been subject to the Data Breach, as the inadequate security measures, discussed *infra*, were the standard Equifax operating method.[3]

B. Equifax Promised to Protect Its Customers' Employees' PII, but Maintained Inadequate Data Security

19. Equifax is one of the major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, including providing services through "The Work Number®, the most extensive source of income and employment information in the U.S. During 2015, we [Equifax] grew that database to include more than 5,000 employers. The Work Number helps

[3] *See quote from Kroger Spokesman Keith Dailey*, http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last accessed May 19, 2016).

individuals obtain credit and other benefits through the verifications of income and employment they provide to lenders, social service agencies and others pursuant to an individual's authorization."[4] As described by Equifax, "[b]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, and human resources-related services. We also offer products that enable individual consumers to manage their financial affairs and protect their identity."[5]

20. With Regard to W-2s in particular, prior to the Data Breach, Equifax explained "[a]s W-2 data is sensitive and subject to federal regulations, every precaution is taken to ensure both security and accuracy. Equifax performs extensive testing and reviews before distribution."[6] Equifax further reassured customers that "Equifax makes it easy to manage administration related to W-2s through web Manager. This user-friendly online tool is seamlessly integrated into all Equifax services, and **can only be accessed by authorized staff members with a valid user ID and PIN.**"[7] (emphasis added)

21. Prior to the Data Breach, Equifax promised its customers and everyone about whom it collects PII that it would reasonably protect their PII. Equifax's privacy policy stated, in relevant part: "We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers."[8]

22. Equifax further cautioned small businesses utilizing its services to "Choose your passwords carefully: ...Don't use your name, address, phone number, initials, Social Security number, license plate or birthday..." [9]

---

[4] *See* 2015 Equifax Annual Report, pg 4 http://files.shareholder.com/downloads/ABEA-32806R/1877079758x0x882810/CC30F45C-8BF7-4814-8A29-A7CE1D85EDCA/15-1002_2015_Annual_Report_Interactive_PDF_FINAL_032116.pdf (last accessed May 19, 2016)
[5] *Id.* at 12.
[6] *See* Equifax, *W-2 Management Truly a win-win situation*, http://www.talx.com/solutions/payreporting/w2/W2_Brochure_EFX.pdf , at 3(last accessed May 19, 2016).
[7] *Id.* at 4
[8] http://www.equifax.com/privacy/ (last accessed May 19, 2016)
[9] http://www.equifax.com/privacy/equifax-small-business (last accessed May 19, 2016)

23. Despite that admonition, Defendant set default passwords and PIN numbers for its W-2 services as the last four digits of individual's social security numbers and the four digit year of birth for those individuals.

24. Plaintiff's and Class Members' PII (in the form of at a minimum their W-2s) was disclosed to Equifax, and Equifax compiled, maintained, and furnished Class Members' PII, in connection with Class Members' acquisition of services, through Defendant's "The Work Number" service. Equifax is allowed to perform such services, involving such sensitive information, only if it adheres to the requirements of laws meant to protect the privacy of such information, such as the Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance, use, and furnishing of such PII is and was intended to affect Plaintiff and other Class Members, and the harm caused by disclosure of that PII in the Data Breach was entirely foreseeable to Equifax.

25. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting businesses who have encountered a data breach.[10]

26. Equifax expressly advises businesses which have lost customer data to "Quickly Notify Those Affected"; "Provide Personalized Communication"; and "Offer Credit Protection."[11] Despite those admonitions, to date, Equifax has not reached out to affected employees, and has not provided personalized communications to those affected, or offered credit protection to those whose W-2s were compromised by the Data Breach.

C. Impact of the Data Breach

27. Since identity thieves use the PII of other people to commit fraud or other crimes, Plaintiff and other consumers whose information was exposed in the Data Breach are subject to a substantial, increased, concrete risk of identity theft. Javelin

[10] *See, e.g.* *http://talx.com/Solutions/Compliance/BreachSolutions/* (last accessed May 19, 2016); http://www.equifax.com/business/equifax-breach-products (last accessed May 19, 2016).
[11] http://talx.com/Solutions/Compliance/BreachSolutions/ (last accessed May 19, 2016).

Strategy & Research, a research-based consulting that specializes in fraud and security in advising its clients, reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (*e.g.*, eBay, Amazon) and email payment accounts such as PayPal."[12]

28. The exposure of Plaintiff's and Class Members' Social Security numbers in particular poses serious problems. Criminals frequently use Social Security numbers to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."[13] Even where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start."[14] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.

29. As a result of the compromising of their personal information, Plaintiff and Class Members have experienced and will face a substantial risk of experiencing the following injuries:

---

[12] *See* https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy (last visited April 14, 2016).

[13] Tips, How to Protect Your Kids From the Anthem Data Breach," Kiplinger (Feb. 10, 2015), *available at* http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited May 19, 2016).

[14] Social Security Administration, Identity Theft and Your Social Security Number, pp. 7-8, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 19, 2016)

- money and time expended to prevent, monitor, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- costs of credit monitoring, as Defendant has offered none to date;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

30. The risks that Plaintiff and Class Members bear as a result of the Data Breach cannot be fully mitigated by credit monitoring because it can only help detect, but will not prevent, the fraudulent use of Plaintiff's and Class Members' PII. Instead, Plaintiff and Class Members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency (such as Equifax) must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiff and Class Members.

D. Equifax Was Required to Investigate and Provide Timely and Adequate Notification of the Data Breach under Federal Regulations

31. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to ***insure the security and confidentiality of customer records and information***;
>
> (2) to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and

> (3) to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b) (emphasis added).

32. In order to satisfy their obligations under the GLBA, financial institutions must "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4. "In order to develop, implement, and maintain [their] information security program, [financial institutions] shall:

> (a) Designate an employee or employees to coordinate [their] information security program.
>
> (b) ***Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information*** that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [their] operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) ***Design and implement information safeguards to control the risks [they] identify through risk assessment***, and regularly

> test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> (d) Oversee service providers, by:
>
> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
>
> (2) Requiring [their] service providers by contract to implement and maintain such safeguards.
>
> (e) ***Evaluate and adjust [their] information security program in light of the results*** of the testing and monitoring required by paragraph (c) of this section; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program."

Id.

33. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* "At a *minimum*, an institution's response program should contain procedures for the following:

> a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
>
> b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
>
> c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement

> authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
>
> d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
>
> e. Notifying customers when warranted.

Id. (emphasis added).

34. Further, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *See id.*

35. Credit bureaus are "financial institutions" for purposes of the GLBA, and are therefore subject to its provisions. *See TransUnion LLC v. F.T.C.*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, *Bank Holding Companies and Change in Bank Control*, "credit bureau services[15]" are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." Since Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

36. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

[15] Credit bureau services include "[m]aintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower." *See* 12 C.F.R. § 225.28.

37. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

38. Upon information and belief, Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" as mandated by the GLBA. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

39. Equifax has also failed to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information, and has failed to communicate directly with Class Members to date.

E. Equifax Failed to Comply with FTC Requirements

40. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines

also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

43. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

44. By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

CLASS ACTION ALLEGATIONS

45. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

46. Plaintiff brings the negligence, negligence per se claims and Declaratory and Injunctive Relief (Counts I, II and IV) on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> *All natural persons and entities in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Kroger on May 5, 2016.*

B. Georgia Subclass

47. Plaintiff brings the state data breach notification claim on behalf of a separate statewide subclass, defined as follows:

All natural persons and entities in Georgia whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Kroger on May 5, 2016.

48. Plaintiff also brings the negligence and negligence per se claims (counts III and IV) separately on behalf of the Georgia Subclass, in the alternative to bringing those claims on behalf of the Nationwide Class.

49. Except where otherwise noted, "Class Members" shall refer to members of the Nationwide Class and the Georgia Subclass, collectively.

50. Excluded from the Nationwide Class and the Statewide Subclass are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

51. The Nationwide and Statewide Subclass meet the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the reasons set forth in Paragraphs 39-47:

52. **Numerosity:** The Nationwide and Statewide Subclass are so numerous that joinder of all members is impracticable. Kroger employees more than 431,000 people, who may be subject to the Data Breach.[16] The parties will be able to identify each member of the Nationwide Class and Statewide Subclass after Defendants' document production and/or related discovery.

53. **Commonality:** There are numerous questions of law and fact common to Plaintiff and the Nationwide and Georgia Subclass, including but not limited to the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their PII;

[16] *See* http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (Last accessed May 19, 2016)

- whether Defendants breached their duties to protect the personal information of Plaintiff and Class member;
- whether Defendants knew or should have known that their data security systems and processes were vulnerable to attack;
- whether Plaintiff and Class member suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII; and
- whether Plaintiff and Class Members are entitled to equitable relief including injunctive relief.

54. **Typicality:** All Plaintiff's claims are typical of the claims of the Nationwide Class, and each Plaintiff's claims are typical of the claims of the Statewide Subclass.

55. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Nationwide Class and Statewide Subclasses. Plaintiff has no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

56. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class and Statewide Subclass predominate over any questions which may affect only individual Class Members in any of the proposed classes, including those listed in paragraph 40, *supra*.

57. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties,

conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

58. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

59. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the PII of the Class Members and other individuals, and varying adjudications could establish incompatible standards with respect to: Defendants' duty to protect individuals' PII; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other Class Members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

60. **Injunctive Relief:** In addition, Defendants have acted and/or refused to act on grounds that apply generally to the Nationwide and Statewide Subclass, making injunctive and/or declaratory relief appropriate with respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the PII of Class Members, and (2) fail to adequately protect their PII.

61. **Certification of Particular Issues:** In the alternative, the Nationwide and Statewide Subclass may be maintained as class actions with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class and the Statewide Subclass)

62. Plaintiff incorporates paragraphs 1-61 as if fully set forth here.

63. Equifax owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information adequately secured from unauthorized access.

64. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Class Member's PII.

65. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

66. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

67. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Member's PII.

68. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach.

69. Equifax had a special relationship with Plaintiff and Class Members from being entrusted with their PII, which provided an independent duty of care. Plaintiff's and other Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

70. Equifax's role to utilize and purportedly safeguard Plaintiff's and Class Members' PII presents unique circumstances requiring a reallocation of risk.

71. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that

Defendants' data security practices were inadequate to safeguard Class Member's PII; and (d) failing to provided adequate and timely notice of the breach.

72. But for Equifax's breach of its duties, Class Member's PII would not have been accessed by unauthorized individuals.

73. Plaintiff and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class Members.

74. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Nationwide Class Member's PII and consumer reports.

75. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Member's PII has also diminished the value of the PII.

76. The damages to Plaintiff and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

77. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE PER SE

(On behalf of the Nationwide Class and the Statewide Subclass)

78. Plaintiff incorporates paragraphs 1-61 as if fully set forth herein.

79. Section 5 of the Federal Trade commission Act ("FTC Act"), 15 U.S.C. § 45 prohibits "unfair...practices in or affecting commerce" including, as interpreted and

enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by businesses such as Equifax of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form the basis of Equifax's duty.

80. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach in their systems, including specifically the immense damages that would result to consumers.

81. Equifax's violation of Section 5 of the FTC Act constitutes negligence *per se*.

82. Members of the Class and Subclass are within the class of persons Section 5 of the FTC Act was intended to protect as they are individuals engaged in trade and commerce, and bear the risk associated with defendant's failure to properly secure their PII.

83. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, have put consumers' personal data at unreasonable risk, causing the same harm suffered by Class Members and Subclass Members.

84. Equifax was further required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> **(1)** to ***insure the security and confidentiality of customer records and information***;
>
> **(2)** to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and

> **(3)** to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer.

85. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4

86. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

87. Further, when Equifax became aware of " unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

88. Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

89. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to,

Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

90. Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

91. Plaintiff and Class Members were foreseeable victims of Equifax's violations of the FTC Act and GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class Members themselves would cause damages to Class Members.

92. Defendants' failure to comply with the applicable laws and regulations, including the FTC Act and GLBA, constitute negligence *per se*.

93. But for Equifax's violation of the applicable laws and regulations, Class Members' PII would not have been accessed by unauthorized individuals.

94. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff and Class Members' PII has also diminished the value of the PII.

95. The damages to Plaintiff and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations.

96. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT III

VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT

Ga. Code Ann. § 10-1-912, *et seq.*

(On Behalf of the Georgia Subclass)

97. Plaintiff incorporates paragraphs 1-61 as if fully set forth herein.

98. Under Ga. Code Ann. § 10-1-912(a), "[a]ny information broker … that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay … ."

99. Under Ga. Code Ann. § 10-1-912(b), "[a]ny person or business that maintains computerized data on behalf of an information broker … that includes personal information of individuals that the person or business does not own shall notify the information broker … of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

100. The Equifax Defendants are information brokers that own or license computerized data that includes personal information, as defined by Ga. Code Ann. § 10-1-911.

101. In the alternative, the Equifax Defendants maintain computerized data on behalf of an information broker that includes personal information that the Equifax Defendants do not own, as defined by Ga. Code Ann. § 10-1-911.

102. Plaintiff's and the Georgia Subclass Members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under Ga. Code Ann. § 10-1-911(6).

103. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Georgia Subclass Member's Personal Information), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

104. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

105. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiff and Georgia Subclass Members suffered the damages alleged herein.

106. Plaintiff and the Georgia Subclass Members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

COUNT IV

DECLARATORY AND INJUNCTIVE RELIEF

(On behalf of the Nationwide Class and the Statewide Subclass)

107. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortuous and which violate the terms of the federal and state statutes described in this complaint.

108. An actual controversy has arisen in the wake of Equifax's data breach regarding its common law and other duties to reasonably safeguard individuals PII. Plaintiffs allege that Equifax's data security measures were inadequate and remain inadequate.

109. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax owed and continues to owe a legal duty to secure Class Members' personal and financial information – specifically

including W-2s of Class Members – and to notify Class Members of a data breach under the common law, Section 5 of the FTC Act and GLBA;

b. Equifax breached and continues to breach this legal duty by failing to employ reasonable security measures to secure Class Members' PII;

c. Equifax's breach of its legal duty proximately caused the data breach which Kroger announced on or about May 5, 2016;

d. Equifax's continued failure to disclose exactly the scope of the data breach, and the individuals effected by the breach makes it impossible for class members to take appropriate measures to mitigate the risk of future identity theft.

110. The Court also should issue corresponding injunctive relief requiring Equifax to employ adequate security protocols to protect the PII of Class Members in its possession. Specifically, this injunction should, among other things direct Equifax to:

a. utilize industry standard secure default password and pin combinations in protecting individuals' PII;

b. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

c. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

d. regularly test its system for security vulnerabilities, consistent with industry standards;

e. immediately notify all Class Members of the data breach, and the scope of PII that was disclosed.

111. If an injunction is not issued, Class Members will suffer irreparable injury and lack an adequate remedy in the event of another data breach, at Equifax. The risk of another such breach is real, immediate, and substantial. If another breach at Equifax

occurs, Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

112. The hardship to the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another data breach occurs at Equifax, the class will likely incur further risk of identity theft and fraudulent use of their PII. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security and notice measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

113. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Equifax, thus eliminating the injuries that would result to Class Members and others whose PII Equifax later obtains whose information would be compromised.

RELIEF REQUESTED

Plaintiff, on behalf of himself and all others similarly situated, request that the Court enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representatives of the Class and Subclass requested herein;

B. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain PII to comply with the, the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how

to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiff and all Class (and Subclass) Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiff and all Class (and Subclass) Members of credit monitoring and identity theft protection services;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

F. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: May 24, 2016

Respectfully submitted,

/s/ Rachel Soffin

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Rachel Soffin
Ga. Bar No. 255074
John A. Yanchunis (pending *pro hac vice* application)
191 Peachtree Street NE, Suite 4200
Atlanta, Georgia 30303
Telephone: (813) 223-5505

Facsimile: (813) 222-2434
jyanchunis@forthepeople.com
rsoffin@forthepeople.com

LOCKS LAW FIRM, LLC
Michael A. Galpern (pending *pro hac vice* application)
Andrew P. Bell (pending *pro hac vice* application)
James A. Barry (pending *pro hac vice* application)
801 N. Kings Highway
Cherry Hill, New Jersey 08034
Tel: (856) 663-8200
Fax: (856) 661-8400